Passenger Name Records – from Canada back to the EU

verfassungsblog.de/passenger-name-records-from-canada-back-to-the-eu/

Raphael Bossong Fr 28 Jul 2017

Fr 28 Jul 2017

The CJEU opinion 1/15 from 26 July, with rejects the EU-Canada PNR agreement has been greeted with cheers from civil rights and privacy advocates.

To recall, the transfer of Passenger Name Records (PNR) held by private airlines to security authorities in order to screen inbound passengers was first required in 2003 by the US. The analysis of extended data generated at the time of booking (full travel itineraries, means of payment, contact details, co-travellers, etc.) has been said to boost the detection previously unknown suspects of terrorism and serious crimes. Over the last decade, this kind of (semi-automated) analysis of PNR data has spread over the OECD world, with traditional US allies of the Five Eyes (Canada, Australia, UK and New Zealand) at the forefront of the trend.

In response, the EU experienced a protracted debate to regularize this transfer of PNR data, including two rebuttals by the ECJ of the initial EU-US PNR agreements in 2004 and 2006. Following on from this, the EU concluded parallel PNR agreements with Australia (2013) and Canada (2014), while negotiations with further countries are likely in the future. For instance, Japan is said to move to PNR analysis ahead of the 2020 Olympics.

Meanwhile, several European member states, led by the UK, have long argued for the necessity of a PNR analysis system of their own. The European Commission started to look into this dossier nearly a decade ago, tabling a formal proposal in 2010. At the time, however, the European Parliament (EP) held many reservations against this proposal, most notably on the grounds that any PNR system collects and retains substantial amounts of information on all passengers, irrespective of individual grounds for suspicion. It took years of negotiation and the shock of several terrorist attacks in France to clear the way for the adoption of an EU PNR Directive in spring 2016 (Directive 2016/681). Yet already in January 2015, the EP had launched a legal challenge to test the validity of the EU-Canada PNR agreement, following on from the previously successful challenges against the EU-US agreement.

The new opinion of the Court of Justice needs to be read against this sensitive political background. The opinion will have major repercussions both for the relations of the EU with partner countries and the development of the EU's own counterterrorism or internal security policy.

To begin with, the opinion (ECLI:EU:C:2017:592) from 26 July underlines the need for precision in the EU's security cooperation with third countries and as well as the importance of including a primary legal basis for data protection, even if the intention of the cooperation is primarily for security purposes. Therefore, security agreements with other third countries will be subject to renewed scrutiny, including in fields beyond PNR (e.g. on the transfer of SWIFT financial transaction data to the US for counterterrorism purposes). For a more in-depth analysis, see the blog entry by Christopher Kuner from 26 July.

Yet arguably the most pressing question for European policy-makers and security authorities is whether the implementation of the EU's own 2016 PNR directive (2016/681) can go ahead as planned. In light of the long and highly contested history of the PNR dossier just touched upon, there are many actors who are eager to upend the measure. The fate of the EU's telecommunications data retention directive and the CJEU judgements on subsequent national legislation (Tele2 Sverige and Watson and Others) at the end of 2016 have given further headwind to critics.

So it is almost certain that the EU's PNR Directive will come next for review before the CJEU, even if the process of implementing the directive and setting up national units in all EU member states for handling PNR data is already underway. It is therefore of critical importance to debate early on, how the last CJEU opinion on the EU-Canada PNR agreement could reflect on this coming legal challenge. For this purpose, the question of the appropriate legal basis of the EU-Canada agreement seems less relevant than the other substantive questions

dealt by the opinion.

With these considerations in mind, the Court opinion seems to suggest:

1. The Court accepts the proportionality of PNR data collection and analysis for the purposes of the prevention and investigation of serious crimes and terrorism. These purposes justify the interference with the right to privacy and basically non-consensual use of PNR data by security authorities. The key expression used repeatedly by the Court is “strictly necessary” (see esp. para 178, 180, 198, 201, 203). This could be good news for proponents of the EU PNR directive.
2. Also the storage and retention of PNR data is accepted by the Court, in so far as it relates to border crossing and specific reasons to conduct an investigation or prevent serious crimes or terrorism as long as the traveler is on the territory of Canada) (para 194, 200, 201, 208)
3. The Court also explicitly referred to the EU PNR Directive as a model to limit the potential for discrimination or collection of especially sensitive data under PNR data exchanges (para 166)
4. In addition, the required clarification on the role of automated analyses (opinion, para 232 3b) in the EU-Canada agreement is probably already fulfilled by the EU PNR directive, which requires human intervention (see Directive2016/681 Art. 12(5))
5. Finally, the Court also has been moved to accept the extended maximum timeframes for data storage of five years (para.209), which is also the specified retention period for the EU PNR directive (Art.12(1))
6. But in contrast to all these conceding points, the Court makes a major distinction between data collected on all passengers that travel to, and stay in, Canada, and the retention and use of data after passengers have left the territory of Canada. This critical point is most strongly worded in the conclusion (para 232 3 c & d), and in arguably a weaker form in the main text of the opinion (para 201-208). While this distinction may appear as a secondary issue, it actually could have serious repercussions for the EU PNR Directive, which does not make such a distinction. The EU Direction only foresees masking/depersonalization procedures of collected PNR data after 6 months from until maximum retention period of five years. (EU PNR Directive Art. 9(2), Art 12.), and makes no reference to the fact whether a person stays in the EU’s territory or not.

While there could be other reasons to test the EU PNR Directive and the respective national implementation measures (e.g. on suitability of data protection authorities, etc.), overlapping EU laws in all these fields could make the case for generally adequate safeguards and oversight mechanisms. Yet the link between data retention and stay on the territory of the EU questions the very foundation of the PNR system, irrespective of the question whether this data is masked or not.

This could mean that any use of PNR data after the respective traveler has left the territory of the EU would require special authorization. For example, a traveler would stay two weeks in the EU, and his or her PNR data would be automatically moved to a different category after exit, where it would only be accessible after special authorization by a court or legally designated authority. (EU PNR Directive Art.12(3)

However, this would not only require a revision of the EU directive as it stands, but generates several practical challenges. The EU would have to link the PNR analysis to the function of a so-called Entry-Exit System (EES) – as exist in the US and in Canada. The EU is currently close to agreeing on a comparable EES, but could take several years to create in practice. Moreover, the current EU proposal on the Entry-Exit system is also logically focused on Third Country Nationals, and would only record their movements, whereas EU citizens are only controlled against hits in the separate Schengen Information System that lists wanted persons (among many other police purposes). However, the EU PNR Directive also covers the collection of data on EU citizens on flights from the EU to third countries. Even with the creation of an EES, the EU would have no readily available mechanism to record the reentry of EU citizens, which could be necessary to document the necessary retention period for PNR data.

An even more radical reading of the Court opinion on the EU-Canada agreement could suggest that all travelers PNR data have to be deleted after their exit is recorded (also amounting to the same linkage & interoperability

challenge with a yet-to-be established EES). This would mean that only in specified cases of reasonable suspicion would PNR data be retained up to five years. This would mostly obviate the need for the interim masking after 6 months, as regulated in the current directive, since one would already deal with a targeted group.

This interpretation corresponds with strict interpretation of the Tele2&Watson judgement, which argued for the need to target information collection and data retention to specific groups. The same line of argument could also be used to challenge the eventual creation of an EU Entry-Exit-System, which could be also be construed as an indiscriminate data collection and retention tool. However, it must be said that such a categorical rejection of data retention on travelers beyond a targeted group of suspects is not a foregone conclusion.

For now, member states will probably move ahead with the implementation of the EU Directive and the creation of national PNR units. The CJEU itself may also become more cautious in subsequent legal challenges, given that it has also avoided confrontation in other contested areas of internal security and Justice and Home Affairs, most notably the validity of Dublin rules in emergency situation. Nonetheless, the last Court opinion on the EU-Canada agreement will trigger a major political and legal debate over the coming months, with key actors in the EP eager to take this forward.

SUGGESTED CITATION Bossong, Raphael: *Passenger Name Records – from Canada back to the EU, VerfBlog,* 2017/7/28, http://verfassungsblog.de/passenger-name-records-from-canada-back-to-the-eu/.